UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/385,591	08/29/1999	GARY L. GRAUNKE	42390.P7573	9395

7590 08/17/2005

ALOYSIUS T C AUYEUNG
BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
7TH FLOOR
12400 WILSHIRE BOULEVARD
LOS ANGELES, CA 90025

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 08/17/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/385,591	GRAUNKE ET AL.	
	Examiner	Art Unit	
	Jung W. Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 June 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *28-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *39-47* is/are allowed.

6)☒ Claim(s) *28-37* is/are rejected.

7)☒ Claim(s) *38* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 28-47 are pending.

2. Applicant in the amendment filed on June 27, 2005 amended claims 28 and 39.

3. Claims 1-27 are canceled.

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Response to Amendment

5. The 35 U.S.C. 112, 2nd paragraph rejections to claims 28 and 39 are withdrawn as the amendments to the claims overcome the 112, 2nd paragraph rejections.

Response to Arguments

6. The following is a response to Applicant's arguments listed on pages 8-11 in the amendment filed on June 27, 2005.

7. In reply to Applicant's argument that the 103(a) rejections of claims 28, 32 and 33 are improper because these rejections are based on an invalid premise, examiner respectfully disagrees. In both the stream encipherment and the block encipherment, the "key-2", as shown in Reference no. 3 of figure 2A, is utilized. Moreover, the difference in utilization of the key as indicated by the Applicant does not invalidate the modification of Feistel with Schneier, since in the block cipher mode as disclosed by

Feistel, the key 2 is combined with a new message block (which corresponds to the random number) using mod-2 addition (Feistel '055, col. 12:57-62) then loaded into the MSR; this additional modulo addition step does not prevent a modification of the Feistel invention using Schneier, which suggests modifying a block cipher key according to a stream cipher key. Hence, the rejections to these claims are proper.

8. Applicant's arguments, see Remarks, pgs. 10-11, with respect to the rejections of claims 38-47, have been fully considered and are persuasive. The 103(a) rejections of claims 38-47 have been withdrawn.

Claim Rejections - 35 USC § 103

9. Claims 28, 32, and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Feistel U.S. Patent No. 4,316,055 (hereinafter Feistel 4,316,055) in view of Schneier Applied Cryptography 2nd Edition (hereinafter Schneier).

10. As per claim 28, Feistel 4,316,055 discloses a combination block/stream encoding apparatus (see Feistel 4,316,055; Title, Abstract) comprising:

a. a block cipher key section to be initialized with a block cipher key, having transformation units to transform the block cipher key (Feistel 4,316,055; col. 5, lines 34-40; Figure 4, Reference Nos. 9, 10, 12, 13 and related text);

b. a data section coupled with the block cipher key section to be initialized with a random number, having transformation units to transform the random

number based on the transformed block cipher key (Feistel 4,316,055; Figure 1, MSR and Transformation Element);

c. a stream cipher key section coupled with the block cipher key section to produce data bits to dynamically modify the random number in the data block section (Feistel 4,316,055; col. 5, lines 31-40; Figure 2A, Reference Nos. 8 and 10, and related text; Figure 3, Reference No. 3 and related text; Figure 4, Reference Nos. 10-13 and related text); and

d. a mapping section to receive the modified random number and the transformed block cipher key and generate a pseudo random bit sequence based on the modified random number and the transformed block cipher key (Feistel 4,316,055; Figure 2a, Reference Nos. 5, 20, 21; Figure 2b, Reference Nos. 22, 23, 24, 25, 26 MSR; Figure 4, Reference Nos. 12-13).

11. Feistel does not expressly teach the stream cipher key section modifying the block cipher key according to a stream cipher key to produce data bits. Schneier teaches an OFB block cipher wherein the block cipher key is modified by values from a shift register, and the modified block cipher key dynamically modifies the value in the data block section. Schneier, pages 203-205, section 9.8. Moreover, since the stream cipher key and the block cipher key are one and the same in Feistel (Feistel, Figure 2a, Reference No. 3), and the values of the shift register in Schneier come from the modified key value derived from the block cipher key, the invention of Feistel modified by Schneier covers a stream cipher key section modifying the block cipher key according to a stream cipher key. It would be obvious to one of ordinary skill in the art

at the time the invention was made to modify the invention of Feistel with the teaching of Schneier wherein the stream cipher key section modifying the block cipher key according to a stream cipher key to produce data bits to dynamically modify the random number in the data block section, since it would be desirous to randomize the block cipher key for a more secure cipher system. Schneier, page 209, "OFG/Counter: Security". The aforementioned cover the limitations of claim 28.

12. As per claims 32 and 33, Feistel 4,316,055 covers a combination block/stream encoding apparatus as outlined above in the claim 28 rejection under 35 U.S.C. 103(a). In addition, the data section is initialized with either plain text or a derived random number. Feistel 4,316,055; col. 12, line 33-col. 13, line 14; col. 10, line 42-col. 11, line 2. The aforementioned cover the limitations of claims 32 and 33.

13. Claims 29-31 and 34-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Feistel 4,316,055 in view of Feistel US. Patent No. 3,798,360 (hereinafter Feistel 3,798,360).

14. As per claims 34-36, Feistel 4,316,055 covers a combination block/stream encoding apparatus as outlined above in the claim 28 rejection under 35 U.S.C. 103(a). Feistel 4,316,055 does not disclose the data section to further include fourth, fifth, and sixth registers wherein substitution units are coupled to an output of the fourth register and an input of the sixth register and linear transformation units are coupled between an

output of the fifth register and an input of the fourth register and an output of the sixth register and an input of the fifth register. However, a step code ciphering system found in Feistel 3,798,360 largely covers these limitations regarding a fourth, fifth, and sixth blocks with the above substitution and transformation relations. Feistel 3,798,360; Figure 1, Reference Nos. 20, 22, 28, Steps 1, 2, 3, 4, 5, 6 and related text; Figures 3a-c and related text, especially 'MANGLER' and 'CONFUSER'. Furthermore, since Feistel 3,798,360 teaches that the segmentation of the data blocks are a matter of design choice (Feistel 3,798,360; col. 3, lines 19-24; col. 4, lines 65-68), the fourth, fifth, and sixth blocks are operatively functional as fourth, fifth, and sixth registers. It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the apparatus of Feistel 3,798,360 to the data section of Feistel 4,316,055 since it enables an efficient and secure ciphering means using substitution and transformation steps as taught by Feistel 3,798,360. Ibid. The aforementioned cover the limitations claims 34-36.

15. As per claims 29-31, Feistel 4,316,055 covers a combination block/stream encoding apparatus as outlined above in the claim 28 rejection under 35 U.S.C. 103(a). Feistel 4,316,055 does not disclose the block cipher key section including first, second, and third registers wherein substitution units are coupled to an output of the first register and an input of the third register and linear transformation units are coupled between an output of the second register and an input of the first register and an output of the third register and an input of the second register. However, it is notoriously well known in the

art for cipher keys to be generated by a cryptographic cipher (devices that are aptly named pseudo-random number generators) since cryptographic ciphers create essentially random strings from non-random strings for encryption purposes. Examiner takes Official Notice that cipher keys are conventionally generated using cryptographic means. Furthermore, the limitations claimed in claims 29-31 are based on cipher means in a key section that are operatively identical to the cipher means in the data section outlined in the claim 34-36 rejections listed above wherein the first, second, and third registers correspond to the fourth, fifth, and sixth registers respectively. It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teachings of Feistel 3,798,360 as outlined in the claim 34-36 rejections above to the key section of the invention covered by Feistel 4,316,055 since it enables means to create cryptographically secure cipher keys as known to one of ordinary skill in the art. The aforementioned cover the limitations of claims 29-31.

16. As per claim 37, Feistel 4,316,055 covers a combination block/stream encoding apparatus as outlined above in the claim 29-31 and 34-36 rejections under 35 U.S.C. 103(a). In addition, the mapping section comprises a plurality of logical gates coupled with a register in the block cipher key section and a register in the data section. Feistel 4,316, 055; Figures 2A, 2B as modified by Feistel 3,798,360; Figure 1, 'ENCIPHER'; see claim rejections 29-31. The aforementioned cover the limitations of claim 37.

Allowable Subject Matter

17. Claims 39-47 are allowed.

18. Claim 38 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

19. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

August 10, 2005

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100